Obtainium.ai

ENGINEERED INTELLIGENCE. REAL IMPACT.

AI Security Risks Every Small Business Owner Should Know

Obtainium.ai LLC

Engineered Intelligence. Real Impact.

The Threat Has Changed — Has Your Business Kept Up?

For years, the biggest cybersecurity nightmares for business owners were ransomware attacks and phishing emails. You knew the enemy. You bought antivirus software, trained your staff not to click suspicious links, and called it a day.

That playbook is no longer enough.

A recent survey of 201 security leaders in the retail and hospitality sectors — industries that look a lot like the small and mid-size businesses we work with every day — found that **71% now cite AI as their single biggest security friction point**. That number surpassed ransomware and phishing combined.

This is not a warning about some distant future. AI tools are already inside your business, used by your employees, and creating new risks you may not even be aware of.

This guide breaks down what those risks actually are, what larger organizations are doing about them, and — most importantly — what you can do right now to protect your business without needing a full-time security team.

Why AI Creates a Different Kind of Security Problem

Traditional threats were relatively predictable. A hacker tries to break in. A phishing email tricks someone into handing over a password. You defend against known attack patterns.

AI introduces uncertainty at a fundamental level. The risks are less about hackers exploiting your systems and more about your own employees — with good intentions — doing things that accidentally expose your data or create compliance gaps.

Here is what that looks like in practice:

Shadow AI: The Tools You Don't Know About

Shadow AI refers to AI tools that employees use on their own, without company approval or oversight. Think of a customer service rep pasting a client's complaint into ChatGPT to draft a reply, or a bookkeeper uploading a spreadsheet of financial records to an AI summarizer.

In the same survey, **56% of security leaders identified shadow AI and employee misuse as a top concern**. The problem is not that employees are malicious — it is that they are trying to be helpful. They find a faster way to do their job and use it, not realizing that data submitted to a

public AI service may be stored, used to train future models, or accessible to the service provider.

For a small business, this can mean:

- Customer records ending up in a third-party AI system you never agreed to
- Proprietary pricing or processes being exposed
- Health or financial data being handled outside of your compliance boundaries

> *The risk is not that your employees are breaking the rules. It is that there are no rules yet.*

Accidental Data Leakage Through Public Tools

This is the most common AI-related security incident, and it is almost always unintentional. **75% of security leaders surveyed named accidental data leakage through public AI tools as their top concern** — making it the number one AI risk on their list.

Public AI tools include anything your team accesses through a web browser — ChatGPT, Claude, Gemini, Perplexity, and dozens of others. When an employee types something into one of those interfaces, that data leaves your building.

For most small businesses, this exposure happens through:

- **Customer data**: Names, contact info, purchase history pasted into prompts
- **Internal documents**: Proposals, contracts, financial records uploaded for summarization
- **Business strategy**: Competitive analysis, pricing models, or growth plans discussed with an AI assistant

The fix is not to ban AI tools — it is to establish clear guidelines about what information should never go into a public AI interface, and to identify approved tools that keep your data private.

What Forward-Thinking Organizations Are Doing

The survey found that **81% of organizations have implemented some degree of AI governance framework** — meaning documented policies for how AI can and cannot be used. Of those, 25% have a fully implemented framework, and 57% have a partial one in place.

That leaves roughly 1 in 5 organizations with no formal AI governance at all. If you are reading

this and nodding, you are not alone — but you are in the minority that is most exposed.

Here is what AI governance actually looks like at the practical level for a small business:

An Acceptable Use Policy for AI

This is the single highest-value thing you can do, and it does not require a lawyer or a security consultant. An acceptable use policy answers three questions:

1. **Which AI tools are approved for use?** (A short list is better than none.)
2. **What types of information can be submitted to those tools?** (For example: internal brainstorming is fine; customer names and contact details are not.)
3. **What do employees do if they are unsure?** (Name a specific person or process to check with.)

A one-page document that answers those three questions, shared with your team, is an AI governance framework. It does not need to be more complicated than that to start.

Using AI to Fight AI Threats

Larger organizations are not just defending against AI threats — they are using AI to detect and respond to them. The survey found:

- **63% use AI for threat detection and analysis**
- **53% use AI to generate security threat reports**
- **44% use AI to automate incident response**

For small businesses, this means the same AI tools that create risk can also be part of your defense. Many modern security platforms now include AI-powered threat detection at price points accessible to businesses without dedicated IT staff.

The Budget Signal: Security Is Getting More Expensive

One finding from the survey is particularly important for small business planning: **nearly 90% of security leaders expect AI-related security budgets to increase**, with 43% predicting significant increases and 46% predicting moderate ones.

Why does this matter to you?

Because security vendors set their prices based on what organizations are willing to pay, and enterprise security budgets drive that market. As AI security becomes a bigger line item at

large companies, the tools designed for that problem will become more sophisticated — and more accessible — over the next 12 to 24 months.

This is also a signal about relative urgency. When 90% of security professionals expect to spend more in a specific area, that area deserves your attention.

> *You do not need to match enterprise security budgets. But you do need a plan.*

A Practical Starting Point for Small Businesses

You do not need to solve every AI security challenge at once. Here is a realistic three-step starting point:

Step 1: Take a 15-Minute AI Inventory

Sit down with your team and answer one question: **what AI tools are people actually using right now?** Include free tools, browser extensions, and anything accessed through a web browser. Most businesses are surprised by how many tools are already in use.

Write them down. This list is the foundation of everything else.

Step 2: Draw One Clear Line

From your inventory, identify the one category of information that is most sensitive in your business. For a healthcare-adjacent business, that might be patient or health data. For a retail shop, it might be customer payment information. For a professional services firm, it might be client strategy documents.

Write one rule: **[This type of information] should never be submitted to an external AI tool.**

Share it with your team. That single rule, communicated clearly, prevents the most common form of accidental data leakage.

Step 3: Designate an AI Point Person

You do not need a Chief Information Security Officer. You need one person — even part-time — who is responsible for staying current on AI tool risks and fielding questions from the rest of the team.

This person does not need technical expertise. They need curiosity, good judgment, and a clear mandate to ask questions before approving new tools.

What This Means for Your Business

The shift from ransomware and phishing to AI as the top security concern is not a trend to watch — it is already here. The organizations that are ahead of this are not necessarily spending more money. They are making intentional decisions about which AI tools they use, what data goes into those tools, and who is responsible for keeping those decisions current.

Small businesses have one advantage that large enterprises do not: you can move faster. A policy that takes a Fortune 500 company six months to implement can be live in your business by next week.

If you want help assessing your current AI security posture or building an AI acceptable use policy for your team, our team works with small businesses at exactly this stage — before a problem occurs, not after.